Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A method comprising:

detecting possible security problems at two or more client locations;

transmitting notice of the possible security problems from the two or more client locations across a network to a home location remotely located from the two or more client locations;

determining, at the home location, an anomaly at one of the client locations based on an analysis of at least the possible security problems at the two or more client locations, in which detecting possible security problems at two or more client locations, transmitting notice of the possible security problems, and determining the anomaly based on the possible security problems occur continuously in real time; and

~~transmitting notice~~ notifying the client locations of the anomaly in real time, including notifying the client locations to update collection of security data to include information about the anomaly. ~~to the client locations at which the possible security problems are detected~~

2. (Original) The method of claim 1 further comprising transmitting notice of the anomaly in real time to other client locations that may communicate with the home location over the network.

3. (Cancelled)

4. (Original) The method of claim 1 further comprising inspecting a packet that arrives at the client location to detect the possible security problem.

5. (Previously presented) The method of claim 1 in which the network comprises a virtual private networks.

6. (Original) The method of claim 1 in which the anomaly includes unauthorized access to the network.

7. (Original) The method of claim 1 in which the anomaly includes unauthorized access of a resource accessible through the network.

8. (Original) The method of claim 1 in which the anomaly includes unauthorized use of resources available through the network.

9. (Currently amended) An article comprising:

a machine-readable medium which contains machine-executable instructions, the instructions causing a machine to:

detect possible security problems at two or more client locations;

transmit notice of the possible security problems across a network to a home location remotely located from the two or more client locations;

determine, at the home location, an anomaly at one of the client locations based on an analysis of at least the possible security problems at the two or more client locations~~, in which detection of possible security problems at the two or more client locations, transmission of notice of the possible security problems, and determination of the anomaly based on the possible security problems occur continuously in real time~~; and

~~transmit notice~~ notify the client locations of the anomaly, including notifying the client locations to update collection of security data to include information about the anomaly ~~in real time to the client locations at which the possible security problems are detected~~.

10. (Original) The article of claim 9 further causing a machine to transmit notice of the anomaly in real time to other client locations that may communicate with the home location over the network

11. (Cancelled)

12. (Previously presented) The article of claim 9 further causing the machine to inspect a packet that arrives at the client location to detect the possible security problem.

13. (Previously presented) The article of claim 9 in which the network comprises virtual private networks.

14. (Original) The article of claim 9 in which the anomaly includes unauthorized access to the network.

15. (Original) The article of claim 9 in which the anomaly includes unauthorized access of a resource accessible through the network.

16. (Original) The article of claim 9 in which the anomaly includes unauthorized use of resources available through the network.

17. (Currently amended) A method comprising:

at a home location in a network, receiving from at least two remote clients indications of possible security problems at the clients; [[and]]

determining, at the home location, an existence of an anomaly at one of the remote clients based on an analysis of at least the indications of the possible security problems at two or more of the remote clients~~, in which receiving indications of possible security problems from the at least two remote clients and determining the anomaly based on the indications of the possible security problems occur continuously in real time~~; and

notifying the remote clients to update collection of security data to include information about the anomaly.

18. (Previously presented) The method of claim 17 further comprising transmitting notice of the existence of the anomaly in real time from the home location to the remote clients.

19. (Previously presented) The method of claim 17 further comprising transmitting notice of the existence of the anomaly in real time from the home location to other remote clients that may communicate with the home location over the network.

20. (Cancelled)

21. (Previously presented) The method of claim 17 further comprising transmitting information from the home location to the remote clients to help the remote clients identify possible security problems.

22. (Original) The method of claim 17 further comprising determining the existence of the anomaly based on at least information regarding previous anomalies.

23-27. (cancelled)

28. (Currently amended) An apparatus comprising:

a server;

a first mechanism accessible by the server to determine an anomaly at one of a plurality of clients based on at least information received from two or more of the clients regarding possible security problems~~, in which the anomaly is determined continuously in real time following receipt of the information from the two or more clients~~; and

a second mechanism accessible by the server to transmit notice of the anomaly in real time over a network to the clients, the notice including notifying the clients to update collection of security data to include information about the anomaly.

29. (Currently amended) The apparatus of claim 28 in which the first mechanism determines the anomaly based on at least information regarding previously determined anomalies.

30. (Currently amended) A system comprising:

two or more client terminals;

a server;

for each of the client terminals,

a first client mechanism accessible by the client terminal to detect a possible security problem at the client terminal,

a second client mechanism accessible by the client terminal to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal, and

a third client mechanism accessible by the client terminal to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems;

a first server mechanism accessible by the server to determine an anomaly at one of the client terminals based on at least information received from the two or more client terminals regarding possible security problems, in which the anomaly is determined continuously in real time following receipt of the information from the two or more clients; and

a second server mechanism accessible by the server to transmit notice of the anomaly in real time over the network to the client terminals at which the possible security problems are detected, the notice notifying the client terminals to update collection of security data to include information about the anomaly.

31. (Original) The system of claim 30 in which the first client mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem.

32. (Original) The system of claim 30 in which the first server mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies.

33. (Original) The system of claim 30 in which the second server mechanism is also configured to transmit notice of the anomaly in real time to other client locations that may communicate with the server over the network.

34. (Previously presented) The system of claim 30 further comprising firewalls located between the client terminals and the server and configured to act as an intermediary for information flowing between the client terminals and the server.

35. (previously presented) The system of claim 34 in which at least one of the firewalls includes a corporate server.

36-39 (Cancelled)

40. (Currently amended) A method comprising:

at a server, receiving from at least two remote clients indications of possible security problems at the clients;

determining, at the server, an existence of an anomaly based on the indications of the possible security problems from the at least two remote clients, in which receiving indications of possible security problems from the at least two remote clients and determining the existence of the anomaly based on the indications of the possible security problems occur continuously in real time;

at least one of collecting information on users by using a human immune mechanism and checking and storing names and addresses associated with security problems by using a fingerprinting mechanism; and

sending in real time, from the server to the remote clients, information for updating firewalls protecting the remote clients to account for the anomaly.

41. (Currently amended) A method comprising:

detecting possible security problems at two or more client locations;

transmitting notice of the possible security problems across a network to a home location remotely located from the client locations;

determining, at the home location, an anomaly at one of the client locations based on the possible security problems by searching for particular information in the anomaly, the particular information including ~~at least one of a network address previously noted as a security~~

~~problem and~~ a particular query or command associated with a known intrusion pattern or technique, in which detecting possible security problems at the two or more client locations, transmitting notice of the possible security problems, and determining the anomaly based on the possible security problems occur continuously in real time; and

transmitting notice of the anomaly in real time to the client locations.

42. (Previously presented) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location, including searching for a successful but unexpected login; and

transmitting notice of the anomaly in real time to the client location.

43. (Cancelled)

44. (Cancelled)

45. (Previously presented) The apparatus of claim 28, further comprising at least one of a human immune mechanism to collect information on users, and a fingerprinting mechanism to check and store names and addresses associated with security problems.

46. (Previously presented) The apparatus of claim 28, further comprising a wide view mechanism to collect and maintain information regarding anomalies reported to the server by the clients.

47. (Previously presented) The apparatus of claim 28, further comprising a statistics mechanism to compute and store records of anomalies.

48. (Canceled)

49. (Previously presented) The method of claim 40, further comprising computing and storing records of anomalies by using a statistics mechanism.

50. (Previously presented) The method of claim 41, further comprising updating, in real time, a firewall protecting the client location to account for the anomaly.

51. (Previously presented) The method of claim 42, further comprising updating, in real time, a firewall protecting the client location to account for the anomaly.

52. (Previously presented) The method of claim 42, in which searching for a successful but unexpected login comprises searching for at least one of a login at an unexpected hour, a login from an unexpected location, and a login from an unexpected user.

53. (Previously presented) The apparatus of claim 28, further comprising a complexity theory mechanism to store and perform complex analysis of anomaly trends.

54. (New) The method of claim 1 wherein the notification includes modifying security procedures at the client locations to account for the anomaly.

55. (New) The method of claim 1, further comprising detecting further possible security problems at the client locations using security data that includes information about the anomaly, transmitting notice of the further possible security problems to the home location, and determining, at the home location, a real security problem at one of the client locations based on an analysis of the security data,

wherein detecting further possible security problems at the client locations, transmitting the further possible security problems, and determining the real security problem at one of the client locations occur continuously in real time.

56. (New) The article of claim 9 wherein the notification includes modifying security procedures at the client locations to account for the anomaly.

57. (New) A method comprising:

receiving, at a server, notice that a new application has been installed at a client; and

sending updated security configuration from the server to the client to account for the newly installed application.

58. (New) The method of claim 57 wherein the updated security configuration provides information to the client about how to examine different installed applications for certain anomalies in different ways.

59. (New) The method of claim 57, further comprising updating security configuration at the server to include knowledge about the newly installed application.